Jurnal Riset Komputer (JURIKOM), Vol. 6 No. 1, Februari 2019
ISSN 2407-389X (Media Cetak)
Hal: 79-84

Implementasi Algoritma Elgamal Dengan Pembangkit Bilangan Prima Lehmann Dan Algoritma Least Significant Bit (LSB) Dengan Cover Image Bitmap Untuk Keamanan Data Text

Edi Rahmansyah

Program Studi Teknik Informatika, STMIK Budi Darma, Medan, Indonesia
Jalan Sisingamangaraja No. 338 Medan, Indonesia

Abstrak

Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut kedalam bentuk acak sehingga isi informasi tersebut tidak dapat dibaca atau dimengerti. Algoritma yang digunakan untuk enkripsi telah mengalami perkembangan, mulai dari algoritma klasik hingga algoritma modern. Akan tetapi enkripsi tetap memiliki kelemahan, salah satunya yaitu hasil dari enkripsi akan menghasilkan karakter acak yang akan menimbulkan kecurigaan bahwa informasi tersebut merupakan informasi yang penting. Kriptoanalisis adalah teknik yang digunakan untuk memecahkan kriptografi, dimana data acak dapat dikembalikan ke data asli, sehingga kriptografi tidak sepenuhnya aman. Karena kekurangan tersebut maka berkembang pula teknik pengamanan data dengan menyisipkan informasi kedalam media seperti gambar ataupun video sehingga informasi tersebut tidak kelihatan, teknik tersebut disebut steganografi. Steganalisis adalah teknik yang digunakan untuk mencari tau apakah suatu gambar memiliki informasi yang disisipkan, sehingga dengan teknik ini steganografi belum sepenuhnya aman.

Kata Kunci: Elgamal, LSB, Pengolahan Citra.

Abstract

Encryption is the process of securing an information by making the information into a random form so that the information content cannot be read or understood. Algorithms used for encryption have evolved, ranging from classical algorithms to modern algorithms. But encryption still has weaknesses, one of which is the result of encryption will produce a random character which will raise suspicion that the information is important information. Cryptanalysis is a technique used to solve cryptography, where random data can be returned to the original data, so cryptography is not entirely safe. Because of these shortcomings, data security techniques are also developed by inserting information into media such as images or videos so that the information is not visible, the technique is called steganography. Steganalysis is a technique used to find out whether an image has information that is inserted, so that with this technique steganography is not fully safe.

Keywords: Elgamal, LSB, Image Processing.

1. PENDAHULUAN

Dengan perkembangan *internet* yang sangat pesat, maka kerahasian data atau informasi merupakan objek yang sangat penting. Banyak pengguna *internet* yang dirugikan karena data atau informasi penting yang mereka miliki jatuh ketangan orang yang tidak bertanggung jawab. Oleh karena itu berkembanglah beberapa teknik pengamanan data atau informasi, diantaranya enkripsi dan steganografi.

Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut kedalam bentuk acak sehingga isi informasi tersebut tidak dapat dibaca atau dimengerti. Algoritma yang digunakan untuk enkripsi telah mengalami perkembangan, mulai dari algoritma klasik hingga algoritma modern. Akan tetapi enkripsi tetap memiliki kelemahan, salah satunya yaitu hasil dari enkripsi akan menghasilkan karakter acak yang akan menimbulkan kecurigaan bahwa informasi tersebut merupakan informasi yang penting. *Kriptoanalisis* adalah teknik yang digunakan untuk memecahkan kriptografi, dimana data acak dapat dikembalikan ke data asli, sehingga kriptografi tidak sepenuhnya aman. Karena kekurangan tersebut maka berkembang pula teknik pengamanan data dengan menyisipkan informasi kedalam media seperti gambar ataupun video sehingga informasi tersebut tidak kelihatan, teknik tersebut disebut steganografi. *Steganalisis* adalah teknik yang digunakan untuk mencari tau apakah suatu gambar memiliki informasi yang disisipkan, sehingga dengan teknik ini steganografi belum sepenuhnya aman.

Penelitian yang dilakukan Eike Kiltz dan Krzysztof Piertzak (2010), dalam *Journal of Centrum Wiskunde and Informatica*, berjudul *Leakage Resilient ElGamal Encryption*. Dalam penelitian ini dijelaskan bahwa banyak terjadi serangan terhadap data user, meskipun data tersebut telah dienkripsi. Dengan menggunakan enkripsi, tidak ada jaminan bahwa data aman, bahkan banyak data yang telah dienkripsi dapat dipecahkan. Dengan banyaknya teknik kriptoanalis yang telah berkembang pada saat ini, maka semakin besar kemungkinan untuk memecahkan sebuah enkripsi. Untuk meningkatkan keamanan informasi dalam berkomunikasi, maka pada skripsi ini akan dibuat program yang menggabungkan enkripsi dan steganografi. Dengan menggunakan program ini maka pesan teks akan dienkripsi, kemudian disisipkan kedalam sebuah file gambar berekstensi *Bitmap*, sehingga pesan tersebut tidak kelihatan. Algoritma yang digunakan untuk enkripsi adalah *ElGamal* dengan pembangkit bilangan prima Lehmann, Sedangkan untuk menyisipkan pesan tersebut kedalam file gambar akan menggunakan algoritma *Least Significant Bit* (LSB).

2. LANDASAN TEORI

2.1 Algoritma Elgamal

Algoritma kriptografi Elgamal merupakan salah satualgoritma kunci asimetris yang didasarkan pada algoritma diskrit.Masalah logaritma diskrit adalahdengan memperhatikan hal berikut. Jika diberikan suatubilangan α, maka menghitung $\delta = \alpha^a \pmod p$ adalahmudah, tetapi jika diberikan suatu bilangan δ, maka untuk menemukan α sehingga $\delta = \alpha^a \pmod p$ adalahpermasalahan yang sulit. Algoritma ini dikembangkanpertama kali oleh ilmuan Mesir Taher Elgamal pada tahun 1985. Algoritma Elgamal adalah suatu kunci publik sistem kripto yang dibuat pada tahun 1985.Algoritma Elgamal digunakan untuk melakukan enkripsi dan tanda tangan digital. Keamanan dari algoritma Elgamal terletak pada sulitnya perhitungan algoritma terpisah pada GF(p) ketika p merupakan bilangan prima yang besar. Algoritma yang terpisah diperlukan dan dianjurkan untuk diimplementasikan pada sistem kripto elgamal[4]

Besaran-besaran yang digunakan pada algoritma Elgamal adalah:

1. p =bilangan prima (tidak rahasia)
2. (p,α,β) = kunci publik
3. γ, =chiperteks
4. a =kunci rahasia
5. m =plainteks
6. k=bilangan acak rahasia
7.α =elemen primitif

2.2 Metode LSB (*Least Significant Bit*)

Metode ini menggunakan citra digital sebagai covertext. Pada susunan bit di dalam sebuah byte (1 byte = 8 bit), ada bit yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti (least significant bit atau LSB). Sebagai contoh byte 11010010, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, dan angka bit 0 (terakhir, digaris-bawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya. Misalkan byte tersebut menyatakan warna merah, maka perubahan satu bit LSB tidak mengubah warna merah tersebut secara berarti. Mata manusia tidak dapat membedakan perubahan kecil tersebut.

3. ANALISA DAN PEMBAHASAN

Untuk dapat memahami kebutuhan sistem dan gambaran tugas-tugas yang akan dikerjakan sistem, maka dilakukan analisis dan perancangan sistem. Dalam analisis dan perancang sistem, akan dilakukan pemodelan rancang bangun sistem yang akan diimplementasikan dalam bentuk nyata. Dalam proses ini akan dilakukan proses penyisipan pesan yang terenkripsi dengan sebuah citra berikut. Adapun prosesnya adalah sebagai berikut :

Gambar 1. Contoh

Pesan yang akan dienkripsi dan disisipkan adalah m, dengan Kunci publik (p = 257, = 3, = 243), Kunci privat (p =257, a=5), sedangkan cover image yang digunakan adalah citra dengan matrix 5x5.
Proses yang terjadi :

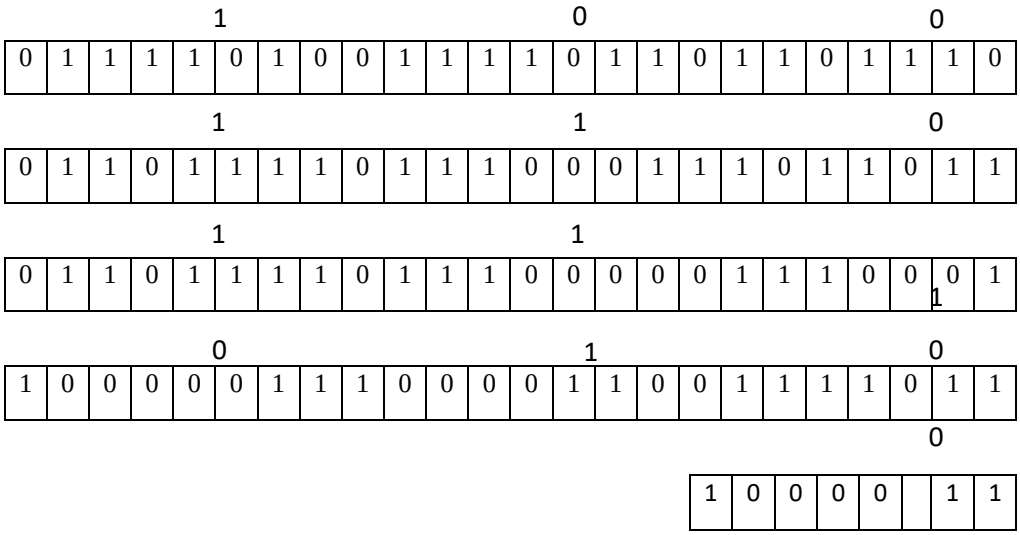
1. Proses enkripsi :
   m = 109, b =7
   $a^b \pmod p$ => $3^7 \pmod{257}$=131
   $ma^{ab} \pmod p$ => $109 \times 131^7 \pmod{257}$=228
   jadi cipertextnya adalah (131,228)
2. Proses penyisipan :

a. Mengubah ciphertext ke binary, binary ciphertextnya adalah 10000011 11100100
b. Mengubah citra menjadi matrix citra dan menghitung byte citra, berikut adalah contoh matrix citranya :

122 123 110	119 113 114	111 113 219	111 112 113	131 134 123
131 134 123	111 112 113	119 113 114	111 113 219	122 123 110
171 134 122	139 144 113	122 123 110	234 234 223	231 124 187
166 234 123	201 204 153	31 34 23	181 224 203	230 134 129
21 144 157	91 84 73	61 184 123	102 103 110	111 104 123

dari matrix pixel dapat dilihat bahwa jumlah pixelnya adalah 25, sedangkan setiap pixel terdiri dari 3 byte, sehingga jumlah bytenya adalah 75.

c. Bandingkan jumlah bit pesan yang akan disisipkan dengan jumlah byte cover, apabila jumlah bitnya lebih kecil atau sama dengan jumlah byte cover, maka proses penyisipan akan dilakukan, jika tidak maka proses dihentikan. 16 < 75, maka proses dilanjutkan.
d. Lakukan proses penyisipan dengan cara mengganti satu bit pesan pada setiap bit kedelapan cover.



e. Setelah disisipi, kemudian jumlah bit disisipkan ke pixel terakhir, maka matrix citranya menjadi berikut :

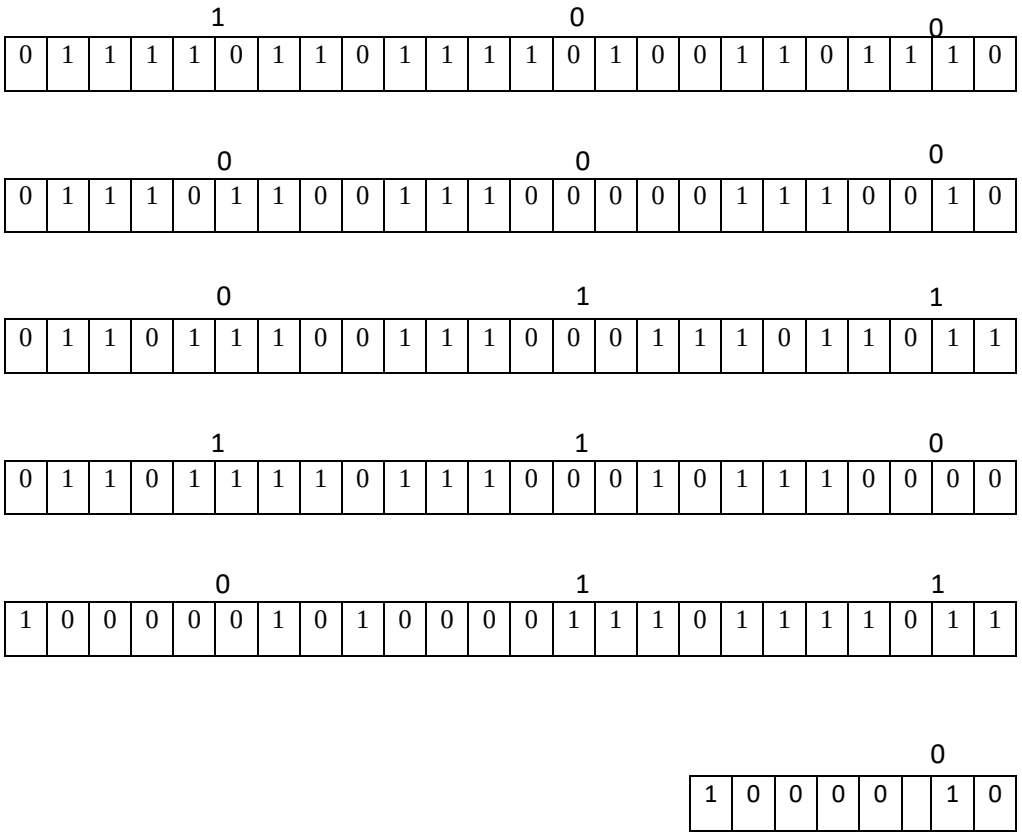
123 122 110	118 112 114	111 112 219	111 113 113	131 135 123
131 134 123	111 112 113	119 113 114	111 113 219	122 123 110
171 134 122	139 144 113	122 123 110	234 234 223	231 124 187
166 234 123	201 204 153	31 34 23	181 224 203	230 134 129
21 144 157	91 84 73	61 184 123	102 103 110	111 104 123

f. Mengubah matrix citra menjadi citra. Berdasarkan contoh diatas dapat diketahui bahwa perubahan terhadap nilai pixelnya adalah kecil dan yang dipengaruhi hanya warna citra. Ukuran dari citra tidak berubah karena yang mempengaruhi ukurannya adalah jumlah matrix citranya.

1. Ekstraksi ciphertext dari citra
   a. Mengubah citra ke matrix pixel dan membaca pixel terakhir untuk mengetahui panjang bit pesan yang disisipi :

123 122 110	118 112 114	111 112 219	111 113 112	131 135 122
131 134 123	110 112 113	119 113 114	111 113 219	122 123 110
171 134 122	139 144 113	122 123 110	234 234 223	231 124 187
166 234 123	201 204 153	31 34 23	181 224 203	230 134 129
21 144 157	91 84 73	61 184 123	102 103 110	111 104 123

b. Mengubah pixel citra ke bit dan mengambil bit kedelapan sebanyak panjang bit pesan yang disisipi, berikut adalah prosesnya :



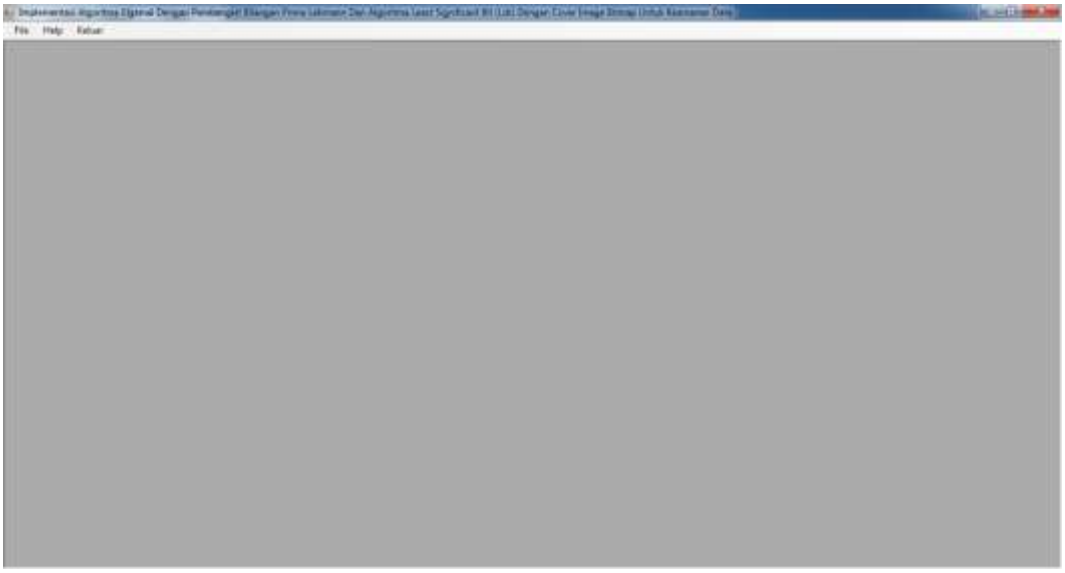
sehingga didapat bit pesan adalah 10000011 11100100.

3. Mengubah bit pesan ke desimal. Bit 10000011 11100100 diubah ke desimal menjadi 131228, sehingga ciphertextnya adalah (131,228)
4. Proses Dekripsi
   Chipertextnya adalah (131, 228) dan kunci privat adalah (p=257, a=5)
   Menghitung
   $(a^b)^{p-1-a}$ (mod p)=> (131) $^{257-1-5}$ (mod 257)=76
   Menghitung
   $(a^b)^{-a}$ ma (mod p)= 76 x 228 mod 257 = 109
   Konversi 109 ke karakter dengan table ascii, sehingga menghasilkan m

4. IMPLEMENTASI

Berikut ini merupakan merupakan tampilan-tampilan yang terdapat di dalam aplikasi yang diuji.

1. Menu Utama
   Adapun hasil eksekusi program ketika pertama kali dijalankan adalah sebagai berikut :



Gambar 2. Tampilan Utama

2. Proses Penyisipan

Proses ini dilakukan dengan terlebih dahulu memasukkan image yang akan digunakan dan diikuti dengan pesan yang akan disembunyikan, setelah itu diikuti dengan penekanan tombol proses yang akan memproses terjadinya penyisipan pesan kedalam citra yang digunakan. Adapun tampilannya dapat dilihat pada gambar 2 dan 3 sebagai berikut:

Gambar 3. Tampilan Awal Proses Penyisipan

3. Proses Ekstraksi

Proses ini digunakan untuk mengekstrak atau menampilkan kembali pesan yang disembunyikan pada citra tersebut. Adapun cara yang digunakan yaitu dengan cara tekan tombol buka gambar pada form tersebut lalu pilih citra yang telah disimpan sebelumnya yaitu hasil penyisipan gmbar dan teks, setelah itu klik tombol proses maka secara otomatis pesan yang disisip sebelumnya akan muncul. Adapun tampilannya dapat dilihat pada gambar 4.dibawah ini.

Gambar 4. Tampilan Proses Pengekstrakan

5. KESIMPULAN

Adapun kesimpulan yang diperoleh dari penulis adalah sebagai berikut:

1. Penyandian pesan dilakukan dengan menggunakan metode Elgamal yaitu penyandian dengan memamfaat kan operasi aritmatik biasa. Dalam tulisan ini Elgamal diimplementasikan untuk menyandikan sebuah pesan agar pesan tidak mudah untuk diketahui oleh pihak lain.
2. Metode LSB (Least significant Bit) dapat diterapkan pada aplikasi penyisipan pesan yang telah di enkripsi pada gambar agar data yang telah diamankan tidak mudah untuk diketahui oleh pihak yang tidak berkepentingan.
3. Aplikasi penyandian dan penyisipan pesan dirancang dengan menggunakan bahasa pemrograman Microsoft Visual Studio 2008 dan telah dapat dijalankan untuk mengamankan data.

REFERENCES

[1] Dony Ariyus, (2008). Pengantar Ilmu Kriptografi. Jogjakarta, Indonesia: Penerbit Andi.
[2] Kusrini, M.kom, (2007). Konsep dan Aplikasi Sistem Pendukung.
[3] Munawar, 2005. Pemodelan Visual dengan UML. Yogyakarta: Penerbit Graha Ilmu.
[4] Utami, Ema dan Sukrisno (2005). Konsep Dasar Pengolahan dan Pemrograman Database dengan SQL Server, Ms. Access, dan Ms.Visual Basic. Yogyakarta: Andi Offset.
[5] Rifki Sadikin, 2012, Kriptografi Untuk Keamanan Jaringan, Yogyakarta
[6] Andi Setyaningsih, Nina (2009). Seri Profesional Pemrograman Visual Basic 2008 Salemba.
[7] Mesran, M. (2012). APLIKASI PENGAMANAN DATA TEKS PADA CITRA BITMAP DENGAN MENERAPKAN METODE LEAST SIGNIFICANT BIT (LSB).